The official voice of the Air Force Research Laboratory
news@afrl
Roundups
April 2002

AFRL awards contract to study system security

by Fran Crumb, Information Directorate

ROME, N.Y. — The Air Force Research Laboratory's Information Directorate has awarded a $120,000 contract to SRI International of Menlo Park, Calif., to conduct a six-month study on the correlation of information system protection reports.

The objective of the study, "Mission-Based Correlation Experiment with AFRL Air Force Enterprise Defense (AFED)," is to prove prototypes for correlating information system protection reports for security incident analysts.

"Intrusion analysis information can be detected, encoded, and reported by various detection engines under development," said Glen E. Bahr, program manager in the directorate's Information Grid Division. "The nature of the cyber intrusion is such that individual event reports may have little meaning until they are correlated with other events across time, across networks, across hardware or software type, or across users and missions."

"The cyber intrusion problem is not like an army breaking into a city; it's more like 1,000 people each entering different portions of a city independently," explained Bahr. "How do you correlate who came at a specific time or place? By watching a bridge, you may only see one person.

With millions of internet 'packets' passing through a system, unless two places know they are being attacked together, you don't realize a coordinated event is underway."

Under the Information Directorate contract, SRI will test the efficacy of certain correlation engines as a prelude to further development of the engines and their integration into more complex systems. The resulting technology could have wide application in computer system security throughout the private and corporate sectors. **@**